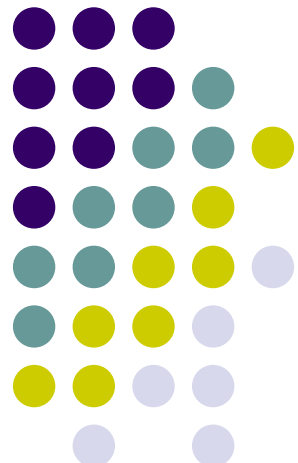
マルチメディア技術

第14回：技術の基礎4

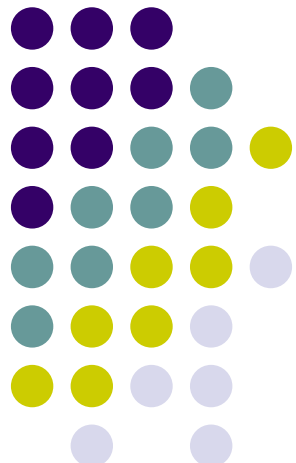


今回話すこと

- インターネットにおけるセキュリティ確保について
- 情報化社会について

セキュリティ

インターネットの安全な応用



セキュリティ

- インターネットを介したサービスの多様化
  - 取引や申請に関わる個人情報や金銭的な情報が誰でもアクセス可能なインターネット上を流れる
- セキュリティ
  - 通信の秘密を守る
  - 通信内容の正当性を保証する
  - 通信相手の正当性を保証する

セキュリティ管理

- インターネットを利用した犯罪
  - 他人の不利をして有料サービスを受ける「なりすまし」
  - 顧客データベースなどの個人情報を不正に販売する「個人情報の流出」
  - ネットワークに侵入してWebページの内容を勝手に変更する「Webページの改ざん」
  - 他人の著作物の利用，他人の誹謗・中傷，虚偽の料金請求
- インターネットを利用することは，こうした犯罪に巻き込まれる危険に常に直面している
  - 日頃から起こりうる危機をあらかじめ予測し，その機器に対する防衛手段を準備しておくこと
  - 危機的情報に陥ったときに即座に的確な対処を取れるように考えておくこと

個人認証

- サービスを受けるユーザが政党であるかどうか確認する
  - ユーザIDとパスワードによる方法
    - パスワードは自分であることを証明する鍵となる
    - 取り扱いには十分注意する
      - 他人に見破られないこと
      - 定期的に変更すること
  - 生体認証
    - 指紋，静脈パターン，網膜パターン

暗号化

- インターネット上で秘密の通信を行う必要があるときは暗号化する
  - 個人情報，金銭情報など
- 暗号化方式
  - 秘密鍵方式
    - 暗号化と複合化に同じ鍵を用い送信側と受信側で共有
  - 公開鍵方式
    - 暗号化鍵と復号化鍵が異なり片方の鍵を公開

秘密鍵暗号方式

メッセージ **This is a pen.**

暗号化鍵 **52314**

暗号化

```
This is a pen.
||||||||||||||
5231452314523 1
||||||||||||||
Yjlt$nu#b$ugq/
```

伝送

暗号文

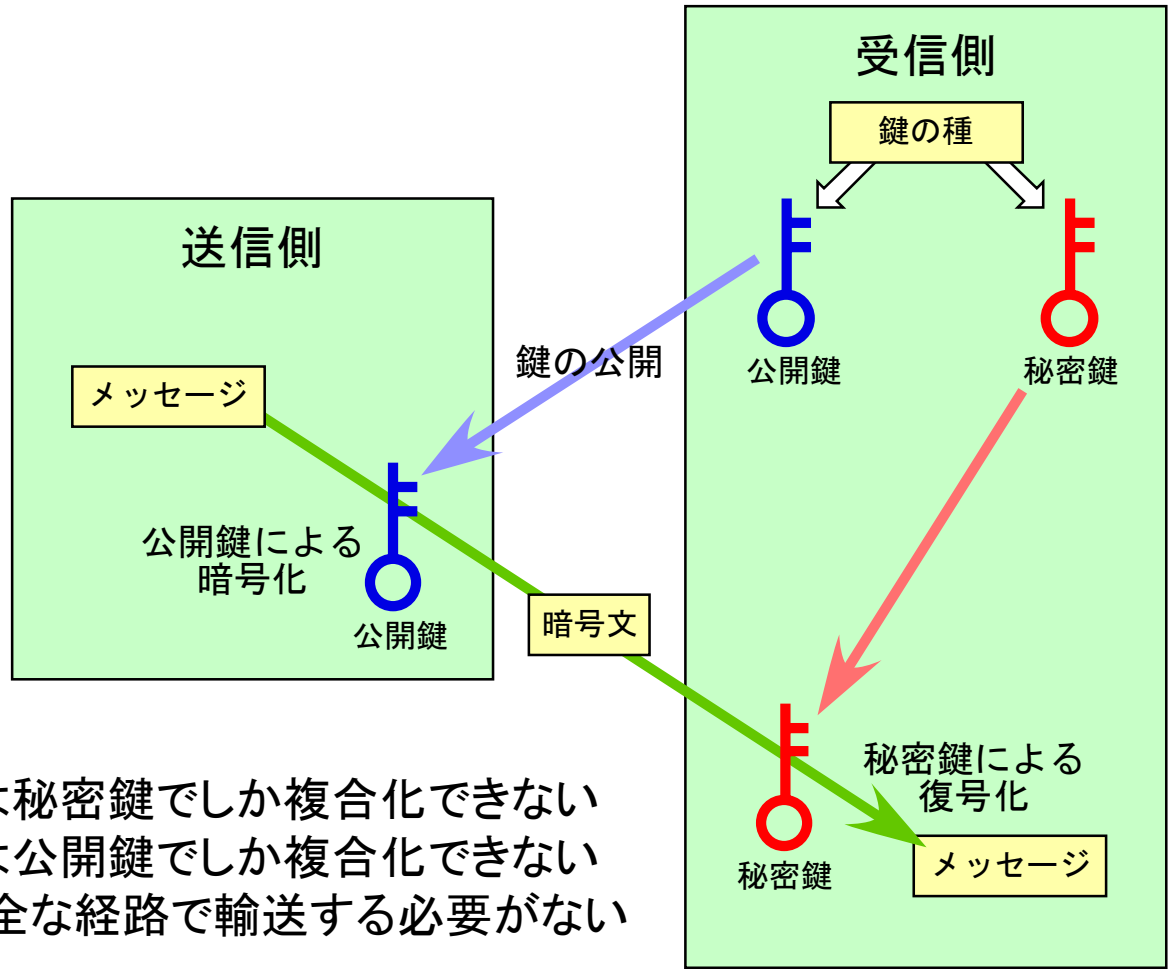
```
Yjlt$nu#b$ugq/
||||||||||||||
5231452314523 1
||||||||||||||
This is a pen.
```

暗号文 **Yjlt$nu#b$ugq/**

暗号化鍵 **52314**

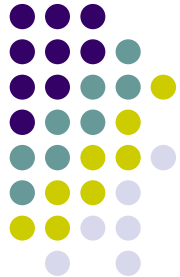
復号化

公開鍵暗号方式



- 公開鍵で暗号化したものは秘密鍵でしか複合化できない
- 秘密鍵で暗号化したものは公開鍵でしか複合化できない
- 秘密鍵方式に比べ鍵を安全な経路で輸送する必要がない

SSL (Secure Socket Layer)



- インターネット上でデータを暗号化して送受信するプロトコル
  - 秘密鍵方式による暗号化を行う
  - 最初に利用者に秘密鍵を送る際には公開鍵方式を用いる
  - 送信データに認証用のコードを付加し受信側でこのコードをチェックしてデータが改ざんされていないか確認する
- Web上で電子商取引など安全な通信を行う必要がある場合に用いられる

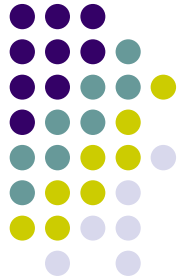
認証局と電子署名

- 認証局
  - 電子商取引やデータ交換を行うものが信用できる相手であることを証明する機関
- 電子署名
  - データに付加された署名であり，認証局が発行する証明書を用いて正当性を確認する
  - 署名を秘密鍵で暗号化し，公開鍵である認証局が発行する証明書を使って複合化できることを確認する

ファイアウォール

- 会社や家庭などのネットワーク (LAN) をインターネットに接続する最，正当な利用目的以外のアクセスを制限する仕組み
  - インターネットから LAN への直接アクセスを遮断する
  - LAN の通信のインターネットへの流出を防止する

コンピュータウィルス

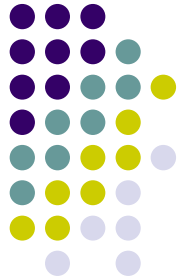


- プログラムの実行により感染するもの
  - 得体の知れないプログラムは実行しない
- 電子メールの添付ファイルとして拡散するもの
  - 得体の知れない添付ファイルは開かない
- Webページの参照により感染するもの
  - 不用意にリンクをクリックしない
  - オペレーティングシステムを最新の状態にしておく
- 自分自身で侵入活動を行うもの（ワーム）
  - オペレーティングシステムを最新の状態にしておく
  - アンチウィルスソフトやファイアウォールを導入する
- 今一番問題になっているのはボット (bot)
  - ワームやトロイの木馬として他人のコンピュータに侵入して，そのコンピュータを遠隔制御できるようにする

コンテンツのセキュリティ

- デジタルデータはコピーが容易
  - 著作権者の意思に反した使用がなされる場合が多い
- 電子透かし
  - ディジタル化された絵画，音楽，映像などのディジタル著作物を不法なコピーや改ざんから守るために，著作物に電子的なコードを埋め込んでおく技術
  - ただし，コピー自体を防止するわけではない

ディジタル著作権管理 (Digital Right Management: DRM)



- 暗号化による著作権保護の機構
  - 著作権のあるデータはメモリカードへのコピー時に公開鍵方式による暗号化を行い不法コピーを防止している
- DVD では
  - CPPM (Content Protection for Prerecorded Media)
    - DVD-ROM 用
  - CPRM (Content Protection for Recordable Media)
    - DVD－RAM／RW（VRモード） 用
  - CCI (Copy Control Information)
    - コンテンツのコピー可／不可の制御，コピー回数の制限

情報モラル

- インターネットの普及
  - 情報の受信者としての役割
  - 情報の発信者としての役割
- 情報の発信者
  - 発信者としての倫理と責任が問われる
  - 不特定の受信者が見ることができるWebページで情報を発信する場合は，意図せず相手に損害を与える場合がある
- 情報の受信者
  - 情報の信憑性を判断できる能力を身に付ける必要がある

ネチケット

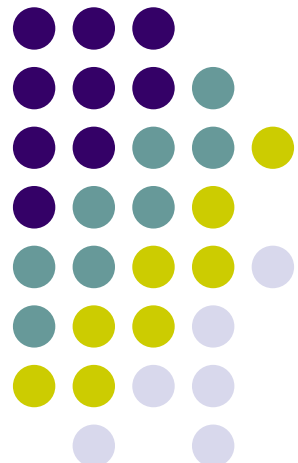
- ネットワーク上のエチケット
- ネチケットガイドライン
  - ガイドラインとして守るべきマナー
  - RFC1855（Request for comments 文書番号1855）

個人情報保護

- プライバシーの保護
  - 個人を特定できる氏名，住所，年齢，電話番号などの情報をみだりに利用したり，公開したりして，個人の人格を損なってはならない
- 個人情報保護法
  - 事業者における個人情報の取り扱いを規制するもの
  - 個人情報の獲得は利用範囲を限定して行う
  - それを逸脱した利用を禁止する
  - 第三者への提供を禁止する
  - 苦情に対しては迅速に対応すべき，など

情報化社会

ITの応用として普及した
サービスや製品について



社会生活の変化

- ディジタルテレビ放送
  - 多チャンネル化，高画質化，双方向機能の実現
    - 地上波アナログ放送は2011年7月で終了（停波）
- 携帯電話
  - 持ち歩ける電話から携帯端末へ
    - Web機能，メール機能，デジタルカメラ機能，音楽再生機能，プログラム実行機能，GPS，・・・
    - 携帯テレビ電話，高速データ通信
- モバイルコンピューティング
  - 場所を選ぶことなくコンピュータを利用できる環境

社会生活の変化

- 情報家電
  - 家庭の電化製品をネットワークで結び，ひとつの端末から状態を把握したり制御したりする
    - テレビ，ビデオなどのAV機器
    - 冷蔵庫，電子レンジ，洗濯機（白物家電）
  - ホームサーバ
    - 端末装置，インターネットと接続して料理のレシピやテレビの番組表のダウンロードを行う

社会生活の変化

- ビデオゲーム機
  - 3次元CGのための専用グラフィックスチップの搭載
    - 動きや視点位置の変更がリアルタイムに行える
  - 大容量記憶デバイスの搭載
    - CD-ROM や DVD-ROM による大規模コンテンツの提供
  - マルチCPU化
    - CG映画に迫る高品質な映像表現の実現
    - 物理シミュレーションやAI（人工知能）の高度化による
ゲームコンテンツ自体のリアル化
    - ブロードバンドネットワーク端子の装備
      - ネットワークゲームへの対応

情報化社会の課題と未来

- 情報格差
  - 情報機器を使いこなせる人と使いこなせない人ではサービスの機会や待遇に不公正さが生じる
- ユニバーサルデザイン
  - 誰にでも使いやすいユーザインタフェースを実現する
    - わかりやすく使いやすくする
    - 視認性の高いボタンのレイアウト
    - 操作ミスを未然に防ぐ機構
  - ユーザビリティを高める
    - 人間の特性を生かした人間工学的な要素の導入

ユニバーサルデザインの7原則

- 誰でも公平に利用できること
- 利用する上での自由度が高いこと
- 使い方が単純で直感的であること
- 必要な情報がすぐに理解できること
- ミスに寛大であり，危険につながらないこと
- 無理を必要とせず，楽に使えること
- 使用しやすい空間と大きさを確保すること

コンピュータ犯罪と法令整備

- インターネットを利用した犯罪の急増
  - 利用者側における危機管理
  - 行政による法規制による犯罪の抑制
- 著作権法
  - プログラムの著作権（1985年）
  - 送信可能化権の設定（1997年）
- 個人情報保護法
- 不正アクセス禁止法
- プロバイダ責任制限法

電子政府

- e-Japan戦略
  - 日本が世界最先端のIT国家になることを目指す基本政策
  - 高度通信ネットワーク社会形成基本法（IT基本法，2000年11月）により決定
  - ネットワークインフラを整備し，マルチメディアを駆使した社会を，国家レベルで推進する
- e-Japan戦略 Ⅱ
  - 進捗状況の見直しや，社会状況の変化に対応するための手直し

ユビキタスネットワーク

- いつでもどこでもネットワークに接続できる
  - 情報機器の増加，多様化
  - 携帯情報機器の普及
  - 駅や街角の店舗でインターネットに接続できる端末の提供
  - 街頭無線LANアクセススポットの整備
- コンピュータそのものを意識せずにITを活用する
  - RFID(ICタグ)
    - 微小な無線チップにより人やモノを識別・管理する仕組み
    - バーコードに代わる商品識別・管理技術として用いられる
    - データは電波等により非接触で読み取ることができる